

High Assurance Multilevel Secure Mail Service: Session Server and IMAP Server

Steven Balmer Susan Bryer-Joyner Brad Eads Scott D. Heller Cynthia E. Irvine
Department of Computer Science
Naval Postgraduate School, Monterey, CA 93943

Orthogonal requirements for security policy enforcement and provision of user-friendly desktop environments have resulted in system architectures unable to satisfactorily meet both objectives. Physical isolation of computers and networks according to sensitivity levels results in duplication and the inability of authorized users who, according to policy, should have access to information to view it. In contrast, it would appear that compatibility with current office productivity software drives out security because popular commercial software packages execute only on untrusted platforms. The high cost of developing multilevel secure platforms precludes their use on every desktop. Architectures are needed that maximize user's ability to view and manage information at different sensitivity levels while still providing high assurance of security policy enforcement.

We are developing a multilevel mail service that combines server-based high assurance mandatory security policy enforcement with commercial-off-the-shelf (COTS) operating systems and software on client systems. The LAN system consists of three principal components. An evaluated high assurance trusted computing base (TCB) is the locus of security policy enforcement and is the mail server platform. COTS PC workstations provide the user's desktop environment. These are not responsible for mandatory security policy enforcement, but may enforce application-specific policies. Last, a Trusted Computing Base Extension (TCBE), installed on the COTS PCs, ensures that a trusted path is established for user identification and authentication as well as certain trusted operations. In addition, the TCBE is intended to control the PC, ensuring object reuse requirements between sessions.

As our high assurance base, we are using the Wang, Inc. XTS-300. To achieve this architecture, we have developed networking components at the TCB to support multiple trusted paths as well as multiple sessions at different sensitivity levels. The result of this effort has been a Secure LAN Server. It provides procedures for the creation of a trusted path between the TCBE and the TCB, over a TCP/IP network; and a framework for utilization of the trusted path for user identification and authentication, and session level negotiation. When combined with the TCBE, the Secure LAN Server creates a TCB interface through which the protocol server, e.g. IMAP, and client applications communicate.

The University of Washington IMAP server has been ported to the high assurance base and has been modified so that, at a particular level, the IMAP instantiation will not only be able to manage mail at that level, but will also be able to view mail at all strictly dominated levels. Thus the clients are provided with a truly multilevel view of mail. No modification of the COTS software providing the client GUI is required, nor are IMAP server instances required to be trusted to enforce the mandatory security policy. Instead each IMAP server instance manages the mail data structures appropriate to its session level. Mail at different sensitivity levels is stored in different folders and these folders are visible at the client GUI, to be provided by a popular COTS mail tool.

Our continuing research to support the Trusted Mail Service involves: development of identification and authentication support in the context of the Secure LAN Server that will take advantage of existing authentication databases of the evaluated TCB; understanding techniques to control the client PC for the purposes of bootstrap, LAN communications control, and object reuse; design of the TCBE executive to support trusted path operations and runtime control of the client PC; and investigation of emerging technologies that may be incorporated into the TCBE in support of trusted path negotiation, communications security, and user identification and authentication.